AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

United States of America
v.
DANUT VALENTIN URSEIU

Case No. 1:24-mj-630

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of January 2023 to February 2023 in the county of Hamilton, Butler in the Southern District of Ohio, the defendant(s) violated:

Code Section	*Offense Description*
Title 18 U.S.C. § 1029	Conspiracy to Commit Access Device Fraud
Title 18 U.S.C. §§ 1344 and 1349	Conspiracy to Commit Bank Fraud

This criminal complaint is based on these facts:

See attached Affidavit.

☑ Continued on the attached sheet.

WESLEY DUN Digitally signed by WESLEY DUN Date: 2024.08.09 09:13:29 -04'00

Complainant's signature

Wesley Dunn, Special Agent

Printed name and title

Received be reliable electronic means and sworn and attested to by telephone.

Date: **Aug 9, 2024**

City and state: **Cincinnati, OH**

Karen L. Litkovitz

Karen L. Litkovitz
United States Magistrate Judge

IN THE UNITED STATES DISTRICT COURT
FOR SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

UNITED STATES OF AMERICA **v.** **DANUT VALENTIN URSEIU**	**Case No.** 1:24-mj-630

AFFIDAVIT IN SUPPORT OF COMPLAINT

I, Wesley Dunn, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am submitting this affidavit in support of the arrest of defendant DANUT VALENTIN URSEIU (URSEIU) for violations of 18 U.S.C. § 1029 (conspiracy to commit access device fraud) and 18 U.S.C. §§ 1344 and 1349 (conspiracy to commit bank fraud) in the Southern District of Ohio, and elsewhere. Specifically, URSEIU conspired with IONUT GIULIANO BOBOC (BOBOC), ANDREI FERNANDO MIHAI DRAMBA (DRAMBA), and others to install and remove "skimmers" on ATM machines in order to steal account information from cardholders and defraud financial institutions of the funds held in the compromised accounts.

2. I have been employed as a Special Agent of the Federal Bureau of Investigation since August 2020, and am currently assigned to the Cincinnati Division. Prior to my employment at the Federal Bureau of Investigation, I was employed for four years as a police

officer at the Owensboro Police Department, located in Owensboro, Kentucky. Additionally, I currently serve in the Indiana National Guard as the Company Commander of the HHD 127th Cyber Protection Battalion. While employed by the Federal Bureau of Investigation, I have investigated federal criminal violations related to high technology or cybercrime, terrorism, money laundering, and credit card fraud. I have gained experience through training at the Federal Bureau of Investigation and everyday work relating to conducting these types of investigations. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

BACKGROUND ON ATM SKIMMERS

4. Law enforcement has been investigating a fraud scheme which utilizes skimming devices ("skimmers") placed on or inside ATMs in the Southern District of Ohio, which acquire debit card information from victims. In addition to the skimmer, the subjects may also install a camera on the face of the ATM to capture entries made by customers on the pin pad of the ATM. This is used to obtain both the card number and corresponding PIN for the card.

5. The skimmer usually does not keep the ATM from otherwise functioning properly. The intended transaction will typically proceed without interruption of any kind or any notification to the victim or third party. Because of this and the fact that the skimmer is installed inside the ATM, it is impossible for victims using the ATM to detect the presence of the skimmer. Additionally, the skimmer does not require a successful transaction to collect the card data; the card data is collected when the victim swipes their card.

6. Based on my training and experience, I know that it is possible to re-encode digitally stored account information onto the magnetic strip of any type of plastic access device using commercially available digital reader-writer devices and the corresponding computer software that comes with the devices. These devices and this software have legitimate commercial uses such as coding hotel room keys and creating security badges.

7. Based on my training and experience, I know that subjects that use fraudulently re-encoded debit cards from ATM skimmers attempt to withdraw cash with the victim's PINs at various financial institution ATMs. The perpetrators can also use prepaid gift cards to re-encode compromised credit card account data onto access devices which they then use to make fraudulent purchases such as additional prepaid credit cards at retail stores.

8. The process of withdrawing cash from ATMs involves the transmission of electronic communications via wire communication between the ATM itself and the bank that holds the compromised account that is being charged for the transaction. These communications are often transmitted in interstate commerce because the various banks are located in different states from each other or the communications sent via wire communications travel interstate based on the locations of the service providers.

9. Through my training and experience, I know ATM skimmers to be devices used to covertly collect debit card data from victims. The illegally collected card numbers are considered access devices. The debit card number related to a victim's account and the cards and card numbers are issued by banks which are federally insured financial institutions. Based on my training and experience, I know individuals involved in ATM skimming will often insert cards after installing a skimmer in order to ensure it was installed correctly.

10. Based on my training and experience I know that individuals sometimes work in groups in furtherance of skimming activity. Once an individual manufactures a skimmer, that individual will use the skimmer in one or more of the following ways: First, the individual can personally use the skimmer to collect card information. Second, the individual can sell the device to another person who will then use the device to collect card information. Third, the individual can provide the device to another person in return for a portion of cards collected by the device as payment. The re-encoded cards can then be used to purchase prepaid goods and services, cashed out, or sold to other individuals.

11. Based on my training and experience I know that individuals involved in skimming sometimes travel from one region to another inserting skimmers, re-encoding cards, and conducting cash out ATM transactions. This sometimes requires individuals involved in skimming to travel with the requisite electronics to conduct skimming activities.

PROBABLE CAUSE

12. On February 4, 2023, a federally-insured U.S. financial institution ("Financial Institution-1") reported to law enforcement that they had identified an ATM skimmer on one of their ATMs in the Southern District of Ohio. On or about February 16, 2023, Financial Institution-1 reported that the number of affected ATM locations had increased to twelve. In all, Financial Institution-1 reported twenty-seven ATM skimming incidents in the first half of 2023, with twenty-three of those incidents falling in the time period URSEIU and his accomplices were known to be operating in the Southern District of Ohio. Financial Institution-1 reported that between the twenty-three locations victimized during that time period there were approximately 3,972 compromised credit or debit card numbers.

13. Financial Institution-1 determined that the first skimmer was installed on an ATM located at 8434 Vine Street in Cincinnati ("ATM-1") on or about January 25, 2023 and that the skimmer compromised 59 credit or debit card numbers. Law enforcement reviewed the surveillance footage obtained from ATM-1, which revealed the following:

a. On January 25, 2023, BOBOC approached the ATM on foot at approximately 11:25pm. BOBOC was observed manipulating the front of ATM-1 and installing a recording device.

14. Financial Institution-1 determined that the next successful skimmer was installed on an ATM located at 1180 Smiley Avenue in Cincinnati ("ATM-2") on or about January 28, 2023, and that the skimmer compromised 180 card numbers. Law enforcement reviewed the surveillance footage obtained from ATM-2, which revealed the following:

a. On January 28, 2023, DRAMBA and BOBOC approached the ATM on foot at approximately 12:25am. DRAMBA and BOBOC appeared to install a device into ATM-2's card reader and a place a camera onto the face of ATM-2.

15. Financial Institution-1 reported another skimmer on an ATM located at 6109 Glenway Avenue in Cincinnati ("ATM-3") on or about February 3, 2023, and that the skimmer compromised 81 card numbers. Law enforcement reviewed the surveillance footage obtained from ATM-3, which revealed the following:

a. On February 3, 2023, URSEIU and DRAMBA approached the ATM on foot at approximately 09:55pm. The subjects were observed manipulating the ATM with URSEIU installing a recording device onto the face of ATM-3.

b. On or about February 23, 2023, the skimmer and camera recovered from ATM-3 were released from the Cincinnati Police Department into FBI custody. On or about April 16, 2024, both devices were released to the Green Township Police Department for latent print examination. On April 25, 2024, a search conducted in latent print databases, IAFIS and OBIS, provided positive identification of URSEIU via latent prints lifted from the back of the camera located on ATM-3. These prints matched prints obtained from URSEIU's 2023 and 2024 arrests for ATM skimming in New York and Michigan.

16. Financial Institution-1 reported another skimmer on an ATM located at 415 Ludlow Avenue in Cincinnati ("ATM-4") on or about February 4, 2023, and that the skimmer compromised 9 card numbers. Law enforcement reviewed the surveillance footage obtained from ATM-4, which revealed the following:

a. On February 4, 2023, DRAMBA approached the ATM on foot at approximately 12:25am. The subject was observed manipulating the ATM installing a recording device into the face of ATM-4.

b. On or about February 23, 2023, the skimmer and camera recovered from ATM-4 were released from the Cincinnati Police Department into FBI custody. On or about April 16, 2024, both devices were released to the Green Township Police Department for latent print examination. On April 25, 2024, a search conducted in latent print databases, IAFIS and OBIS, provided positive identification of DRAMBA via the latent print lifted from the camera recovered from ATM-4.

These prints matched prints obtained from DRAMBA's 2024 arrest for ATM skimming in Michigan.

17. Financial Institution-1 reported another skimmer on a drive-thru ATM located at 7405 N. Liberty Drive in Liberty Township ("ATM-5") on or about February 4, 2023, and that the skimmer compromised 500 card numbers. Law enforcement performed latent print examination of the devices obtained from ATM-5, the results of which were provided to the latent print examiner at the Green Township Police Department. Latent print comparison in the IAFIS and OBIS databases, identified prints that were a match for URSEIU. These prints matched prints obtained from URSEIU's 2023 and 2024 arrests for ATM skimming in New York and Michigan.

18. On or about March 17, 2023, in New York, the Monroe County Sheriff's Office (MCSO) became involved in an ATM skimmer investigation. Between March 9, 2023, and March 23, 2023, incidents of ATM skimming occurred at various branches of ESL Federal Credit Union (ESL) and Canandaigua National Bank (CNB), all of which were located in or around Monroe County, New York. Surveillance footage provided by the affected banks revealed the same individuals installing or attempting to install ATM skimmers at the victimized locations. Surveillance images depicting URSEIU, DRAMBA, and BOBOC were provided by MSCO. Additionally, MCSO provided documentation released by CNB and ESL which revealed the following:

a. CNB reported an estimated loss of $134,000 dollars across approximately 309 compromised cards.

b. ESL did not provide a loss estimate, but reported approximately 377 compromised cards.

19. On or about March 24, 2023, URSEIU, BOBOC, and Radeck Bohdan were apprehended by MSCO in Monroe County New York after they were observed attempting to install a skimmer on an ESL ATM. MSCO seized cell phones belonging to all three suspects and forensic images of each were provided to the FBI. A review of the devices seized from URSEIU and BOBOC revealed the following information:

a. URSEIU's devices:

i. Device location information placing URSEIU in the SDOH during the aforementioned timeframe of skimming incidents

ii. Photos of ATM skimming devices, recording devices, and large amounts of United States currency

iii. Various chat messages with discussions involving ATM skimming activity

b. BOBOC's device:

i. A video depicting two camera variations (clear acrylic and chrome strip.) The chrome strip appears visually similar to the evidence item obtained from ATM-5 and the acrylic device is visually similar to evidence items obtained from ATM-1 and ATM-4.

ii. A photograph of URSEIU, BOBOC, and Radeck Bohdan at what appears to be a restaurant.

iii. Photographs of large amounts of United States currency

iv. Numerous communications with phone number +13123128078, which was the phone number associated with the cellphone seized from URSEIU.

20. On or about February 2, 2024, URSEIU and DRAMBA were arrested near Royal Oak, Michigan in relation to ATM skimming activity. The arrest followed a string of ATM skimming incidents occurring near Detroit, Michigan to include both Troy and Royal Oak Michigan.

21. Throughout the investigation, I was able to positively identify URSEIU, DRAMBA, and BOBOC as they appeared in surveillance footage upon review of booking photos, provided by MCSO and the Troy Police Department, and/or images obtained from a review of URSEIU and BOBOC's cellphones.

CONCLUSION

22. I submit that this affidavit supports probable cause for a warrant to arrest DANUT VALENTIN URSEIU for violations of 18 U.S.C. § 1029 (conspiracy to commit access device fraud) and 18 U.S.C. §§ 1344 and 1349 (conspiracy to commit bank fraud) in the Southern District of Ohio and elsewhere.

Respectfully submitted,

WESLEY DUN Digitally signed by WESLEY DUN Date: 2024.08.09 09:13:03 -04'00'

Wesley Dunn
Special Agent, Federal Bureau of Investigation

Subscribed and sworn to before me on August 9, 2024

Karen L. Litkovitz
United States Magistrate Judge